associating a first policy of a first model set in a first package with a first table within the database system; and

invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy.

A1. Cncld

7. (Amended) A method according to Claim 6, further comprising the step of forming said each package of said one or more packages so that the access mediation routine conforms to a specified interface for enforcing a policy in the database management system.

8. (Amended) A method according to Claim 7, said step of forming said each package further comprising including one or more administrative routines for defining a policy for the model set.

A2

11. (Amended) A method according to Claim 10, said step of invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy.

A3

19. (Amended) A method according to Claim 6, wherein.

the method further comprises the step of determining a set of allowed labels for the first policy for a user of the database management system;

said step of invoking the access mediation routine is performed during said step of determining the set of allowed labels; and

the user is allowed to operate on the data according to the first policy if the data is associated with a label for the first policy and the label is included in the set of allowed labels for the first policy.

A4

26. (Amended) A computer-readable medium carrying one or more sequences of instructions for managing access to data in a database based on a database policy set of one or more label-based security policies, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

registering, with a database management system, one or more packages of routines, wherein each package of said one or more packages implements a security model that supports a model set of one or more policies of the database policy set and said each package includes an access mediation routine;

associating a first policy of a first model set in a first package with a first table within the database system; and

invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy.

A5.

28. (Amended) A computer-readable medium according to Claim 27, wherein said each package of said one or more packages includes one or more administrative routines for defining a policy for the model set.

A6

31. (Amended) A computer-readable medium according to Claim 30, said step of invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy.

A7

39. (Amended) A computer-readable medium according to Claim 26, wherein.

execution of the one or more sequences of instructions further causes the one or more processors to perform the step of determining a set of allowed labels for the first policy for a user of the database management system;

said step of invoking the access mediation routine is performed during said step of determining the set of allowed labels; and

the user is allowed to operate on the data according to the first policy if the data is associated with a label for the first policy and the label is included in the set of allowed labels for the first policy.

Attached hereto is a marked-up version of the changes made to the specification by the current amendment. This attached page is captioned "**Version with Markings to Show Changes Made**."

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: January 30, 2003

Marcel K. Bingham
Reg. No. 42,327

1600 Willow Street
San Jose, California 95125-5106
Tel: (408) 414-1080, ext. 206
Fax: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Washington, D.C. 20231.

on January 30, 2003 by Trudy Bagdon
Trudy Bagdon

Version with Markings to Show Changes Made

1. (Not Amended) A method for managing access to data in a database subject to a plurality of label-based security policies, the method comprising the steps of:

receiving, within a database management system, a request for performing an operation set of one or more operations on data in a table of the database;

determining which policies, of the plurality of label-based policies, apply to the table based on a policy set of one or more policies associated with the table; and

for each operation in the operation set, determining whether to perform the operation on a row of the table based on a set of labels associated with the row, the set of labels corresponding to the policy set.

2. (Not Amended) A method according to Claim 1, further comprising adding a policy column to the table for each policy in the policy set associated with the table

3. (Not Amended) A method according to Claim 2, further comprising storing a label, of the set of labels associated with the row, in a corresponding policy column of the row.

4. (Not Amended) A method according to Claim 2, said step of determining which policies apply further comprising the step of determining whether a column is a policy column.

5. (Not Amended) A method according to Claim 1, wherein the policy set associated with the table includes two or more policies of the plurality of label-based policies.

6. (Amended) A method for managing access to data in a database based on a database policy set of one or more label-based security policies, the method comprising the steps of:

registering, with a database management system, one or more ~~package~~ packages of routines, wherein each package of said one or more packages implements a security model that supports a model set of one or more policies of the database policy set and said each package includes an access mediation routine;

associating a first policy of a first model set in a first package with a first table within the database system; and

invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy.

7. (Amended) A method according to Claim 6, further comprising the step of forming said each package of said one or more packages so that the access mediation routine conforms to a specified interface for enforcing a policy in the database management system.

8. (Amended) A method according to Claim 7, said step of forming ~~the~~ said each package further comprising including one or more administrative routines for defining a policy for the model set.

9. (Not Amended) A method according to Claim 8, said step of including one or more administrative routines for defining a policy further comprising including one or more administrative routines for defining a name for a particular policy; labels for the particular policy; descriptions for the labels; and properties for the labels.

10. (Not Amended) A method according to Claim 6, further comprising the step of invoking an administrative routine of the first package for defining the first policy.

11. (Amended) A method according to Claim 10, said step of invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy.

12. (Not Amended) A method according to Claim 6, further comprising, in response to attempts to operate on data in a row in the table, the step of determining that the first policy applies to the table.

13. (Not Amended) A method according to Claim 6, further comprising the steps of:

associating a second policy of a second model set in a second package with a second table within the database system; and

invoking the access mediation routine in the second package for determining whether to allow operation on data in the second table based on the second policy.

14. (Not Amended) A method according to Claim 13, wherein the second model in the second package is the same as the first model in the first package.

15. (Not Amended) A method according to Claim 13, wherein the second model in the second package is different from the first model in the first package.

16. (Not Amended) A method according to Claim 13, wherein the second table is the same as the first table.

17. (Not Amended) A method according to Claim 13, wherein the second table is different from the first table.

18. (Not Amended) A method according to Claim 6, said step of invoking the access mediation routine in the first package further comprising providing data indicating the first policy to the access mediation routine.

19. (Amended) A method according to Claim 6, wherein.

the method further comprises the step of determining a set of allowed labels for the first policy for a user of the database management system;

said step of invoking the access mediation routine is performed during said step of determining the set of allowed labels; and

the user is allowed to operate on the data according to the first policy if the data is associated with a label for the first policy and the label is included in the set of allowed labels for the first policy.

20. (Not Amended) A method according to Claim 19, further comprising the step of storing the set of allowed labels in a session cache for a communication session between the database management system and the user.

21. (Not Amended) A computer-readable medium carrying one or more sequences of instructions for managing access to data in a database subject to a plurality of label-based security policies, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving a request for performing an operation set of one or more operations on data in a table of the database;

determining which policies, of the plurality of label-based policies, apply to the table based on a policy set of one or more policies associated with the table; and for each operation in the operation set, determining whether to perform the operation on a row of the table based on a set of labels associated with the row, the set of labels corresponding to the policy set.

22. (Not Amended) A computer-readable medium according to Claim 21, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of adding a policy column to the table for each policy in the policy set associated with the table

23. (Not Amended) A computer-readable medium according to Claim 22, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of storing a label, of the set of labels associated with the row, in a corresponding policy column of the row.

24. (Not Amended) A computer-readable medium according to Claim 22, said step of determining which policies apply further comprising the step of determining whether a column is a policy column.

25. (Not Amended) A computer-readable medium according to Claim 21, wherein the policy set associated with the table includes two or more policies of the plurality of label-based policies.

26. (Amended) A computer-readable medium carrying one or more sequences of instructions for managing access to data in a database based on a database policy set of one or more label-based security policies, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps

of:

registering, with a database management system, one or more ~~package~~ packages of routines, wherein each package of said one or more packages implements a security model that supports a model set of one or more policies of the database policy set and said each package includes an access mediation routine;

associating a first policy of a first model set in a first package with a first table within the database system; and

invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy.

27. (Not Amended) A computer-readable medium according to Claim 26, wherein the access mediation routine conforms to a specified interface for enforcing a policy in the database management system.

28. (Amended) A computer-readable medium according to Claim 27, wherein ~~the package~~ said each package of said one or more packages includes one or more administrative routines for defining a policy for the model set.

29. (Not Amended) A computer-readable medium according to Claim 28, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of defining a name for a particular policy; labels for the particular policy; descriptions for the labels; and properties for the labels.

30. (Not Amended) A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more

processors to perform the step of invoking an administrative routine of the first package for defining the first policy.

31. (Amended) A computer-readable medium according to Claim 30, said step of invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy.

32. (Not Amended) A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform, in response to attempts to operate on data in a row in the table, the step of determining that the first policy applies to the table.

33. (Not Amended) A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the steps of:

associating a second policy of a second model set in a second package with a second table within the database system; and

invoking the access mediation routine in the second package for determining whether to allow operation on data in the second table based on the second policy.

34. (Not Amended) A computer-readable medium according to Claim 33, wherein the second model in the second package is the same as the first model in the first package.

35. (Not Amended) A computer-readable medium according to Claim 33, wherein the second model in the second package is different from the first model in the first package.

36. (Not Amended) A computer-readable medium according to Claim 33, wherein

the second table is the same as the first table.

37. (Not Amended) A computer-readable medium according to Claim 33, wherein

the second table is different from the first table.

38. (Not Amended) A computer-readable medium according to Claim 26, said step of invoking the access mediation routine in the first package further comprising providing data indicating the first policy to the access mediation routine.

39. (Amended) A computer-readable medium according to Claim 26, wherein.

execution of the one or more sequences of instructions further causes the one or more processors to perform the step of determining a set of allowed labels for the first policy for a user of the database management system;

said step of invoking the access mediation routine is performed during said step of determining the set of allowed labels; and

the user is allowed to operate on the data according to the first policy if the data is associated with a label for the first policy and the label is included <u>in </u>the set of allowed labels for the first policy.

40. (Not Amended) A computer-readable medium according to Claim 39, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of storing the set of allowed labels in a session cache for a communication session between the database management system and the user.